Response from the Association for Progressive Communications to the 2019 IGF Best Practices forum on Cybersecurity Call for Contributions

Contact: Deborah Brown deborah @ apc.org
www.apc.org

QUESTIONS

1. Is your organization a signatory to any of the agreements covered, or any other ones which intend to improve cybersecurity and which our group should look at? (please specify) If not, we are still interested in your opinion on the rest of this questionnaire!

Freedom Online Coalition Recommendations for Human Rights Based Approaches to Cybersecurity
Global Commission on the Stability of Cyberspace norms

2. What projects and programs have you implemented or have seen implemented to support the goals of any agreements you signed up to? Do you have any plans to implement specific projects?

- *APC is implementing a project called "Putting cybersecurity on the rights track" that is aligned with the recommendations of the Freedom Online Coalition's Recommendations (the "free and secure" recommendations.*
- *APC is involved with others in civil society and the GCSC in follow up on the GGE norms, including facilitating civil society awareness and participation in the current GGE and OEWG.*

3. During our review, we identified a few key elements that were part of multiple agreements and seem to have more widespread support and/or implementation. Do you have views around the relative importance of these (e.g. by providing a ranked list), or are there any others that you consider to be significant commitments in these types of agreements?

We would prioritise these elements as follows (starting with the most important):

- *Reference to Human Rights*: whether the agreement reflects on the importance of human rights online.
- *References to content restrictions*: whether the agreement discusses the need for content restrictions online.

- *Reference to International Law*: whether the agreement reflects on the importance of aligning international law.
- *Reference to Capacity Building*: whether the agreement makes specific references to Capacity Building as a needed step to improve cybersecurity capability.
- *Furthers multi-stakeholderism*: identify or support that cybersecurity depends on the presence in debate and coordination of all stakeholder groups.
- *Responsible disclosure*: the need to coordinate disclosure of security issues between all stakeholders, including the finder, vendor and affected parties.
- *Vulnerability equities processes*: the realization that stockpiling of vulnerabilities may reduce overall cybersecurity, and processes can be implemented to help identify the appropriate course of action for a government when it identifies a vulnerability.
- *Definition of Cyber threats*: whether the agreement proposes a clear or aligned definition of cyber threats.
- *Definition of Cyber-attacks*: whether the agreement proposes a clear or aligned definition of cyber attacks.
- *Specified CBM's*: whether the agreement describes or recommends specific Confidence Building Measures.

4. What has the outcome been of these agreements? Do you see value in these agreements either as a participant, or as an outsider who has observed them?

Yes, there is value in many, if not all, of these initiatives. The value lies as much in the process of formulating these "agreements" as it does in the substantive content of the agreements. As threats in cyberspace are becoming more commonplace and severe, these agreements provide valuable common footing to reduce risk and increase security and stability in cyberspace.

- *Norms are shared beliefs held within a community which relevant actors identify with in order to generate "the pull to conform" to those norms.*
- *Norms are valuable as policy tools. "By clarifying responsibilities and who should do what, norms create obligations for identifiable actors and trigger more active accountability than principles do.""*
- *Norms can eventually evolve into (or inform) laws which would be binding, as opposed to voluntary and non-binding. In practice laws that codify norms which are already understood and accepted by those affected by them, are more likely to be respected, while laws which codify norms which are not widely shared, are more likely to be broken.*

5. Have you seen any specific challenges when it comes to implementing the agreement?

There are a number of challenges when it comes to implementing agreements:

- *Varied understandings or definitions of the key terminology referred to in the agreements (e.g. what is critical infrastructure)*
- *Varied levels of knowledge of the existence of these agreements or norms among states and other stakeholders, as well as capacity to implement them*
- *Challenges in monitoring compliance and implementation because of a lack of institutional capacity and mechanisms that can do the monitoring*
- *The flouting of norms and agreements by influential states that called for them, which acts as a disincentive for others to comply with them*
- Lack of continuity. Often interaction and broader consultation processes stop once the agreement has been reached or published. Ongoing interaction an

6. Have you observed adverse effects, or tensions from any of the elements of these agreements, where specifics may be at odds with intended end results? For instance a commitment that may seem like it improves cybersecurity at first sight or tries to fix one issue, but has effects that lead to a reduction in cybersecurity?

The tendency for cybersecurity agreements to either directly, or indirectly, undermine human rights, which, in our view, reduces cybersecurity. This is a result of cybersecurity frameworks focusing only on the security of the state, rather than the security of people, devices, networks and underlying infrastructure. Such narrow views of cybersecurity tend to call for disproportionate measures, like undermining encryption, which may appear to strengthen national security, but in fact undermine human rights and also the security of society at large.

Another adverse effect is, as mentioned above, that powerful states who are part of these agreements (the GGE and FoC for example) flout them in practice, thereby undermining not just those specific agreements, but international agreements as a mechanism to achieve cybersecurity in the first place.